

張貼日期：2022/07/27

# 【資安漏洞預警】VMware vCenter Server權限提升漏洞CVE-2021-22048請儘速確認並進行更新！

- 主旨說明VMware vCenter Server權限提升漏洞CVE-2021-22048請儘速確認並進行更新！
- 內容說明：
  - 轉發 科學園區資安資訊分享與分析中心 SPISAC-ANA-202207-0008
  - CrowdStrike於去年11月發現遠端攻擊者可利用這個漏洞CVE-2021-22048於目標系統觸發權限提升。
  - VMware近日發布了vCenter Server 7.0 Update 3f來修補這項漏洞，而其他版本用戶則建議依照先前提提供的漏洞緩解指南，將單一簽入SSO的組態從IWA移轉為透過LDAP身分驗證的AD目錄架構。
- 影響平台：
  - VMware vCenter Server 6.7 及 7.0 版本
  - VMware Cloud Foundation (vCenter Server) 3.x 及 4.x 版本
- 建議措施VMware vCenter Server 7.0 版本更新至3f其餘版本則建議依照先前提提供的漏洞緩解指南<https://kb.vmware.com/s/article/86292>
- 參考資料：
  1. <https://kb.vmware.com/s/article/86292>
  2. <https://www.bleepingcomputer.com/news/security/vmware-patches-vcenter-server-flaw-disclosed-in-november/>

計算機與通訊中心  
網路系統組 敬啟

From:  
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:  
[https://net.nthu.edu.tw/netsys/ mailing:announcement:20220727\\_03](https://net.nthu.edu.tw/netsys/ mailing:announcement:20220727_03)



Last update: **2022/07/27 14:33**